REMARKS

Applicants respectfully request that the above-identified application be re-examined.

The November 30, 2009, Office Action ("Office Action") rejected Claim 4 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter that applicants regard as their invention. The specific grounds for the rejection were the inclusion of the words "the data" in the last line of Claim 4. Remarks accompanying this rejection note that there is insufficient antecedent basis for this limitation in the claim and that the claim is not specific as to whether the data that is to be sent is data that is generated from the biometric information or other data that is generated to send after user authentication. In this regard, Claim 4 has been amended to address this rejection. Applicants respectfully submit that Claim 4, as amended, obviates this ground of rejection. As a result, it will not be further discussed.

The Office Action also objected to Claim 1 due to its use of both the term "network connection function" and the term "network connection means." This amendment addresses this objection by changing both terms to network connector. Applicants respectfully submit that this amendment obviates this ground of rejection and, thus, it will not be further discussed.

The Office Action also rejected Claims 1–3 under 35 U.S.C. § 103(a) as being unpatentable in view of the teachings of U.S. Patent Application Publication No. 2003/0214779 ("Socolofsky") taken in view of the teachings of U.S. Patent Application Publication No. 2003/0005336 ("Poo"). Claims 5–6 were rejected under 35 U.S.C. § 103(a) as being unpatentable in view of the teachings of Socolofsky and Poo taken further in view of the teachings of U.S. Patent Application Publication No. 2003/0157959 ("Makela"). Finally, Claim 4 was rejected under 35 U.S.C. § 103(a) as being unpatentable taken in view of the teachings of Socolofsky and Poo taken further in view of the teachings of U.S. Patent

Application Publication No. 2002/0186838 ("Brandys"). While applicants respectfully disagree with the foregoing grounds of rejection, in order to advance the prosecution of this application, Claim 1, the only independent claim in this application, has been amended to better distinguish the claimed subject matter from the teachings of the cited and applied references, in particular, Socolofsky.

Prior to discussing in detail why applicants believe that all of the claims in this application are patentable in view of the teachings of the cited and applied references, a brief description of the disclosed subject matter and brief descriptions of the teachings of the cited and applied references are provided. The following discussions of the disclosed subject matter and the cited and applied references are not provided to define the scope or interpretation of any of the claims of this application. Instead, these discussions are provided solely to assist the U.S. Patent and Trademark Office in recognizing the differences between the pending claims and the cited references and should not be construed as limiting on the disclosed subject matter.

Disclosed Subject Matter

A portable personal server device suitable for functioning as a server when connected to an external network is disclosed. The portable personal server device comprises a local server, a network server, memory, a messaging API, an individual authenticator, and a control. The local server processes data between the portable personal server device and a communication terminal equipped with a local network connector suitable for connection to the portable personal server device. The network server processes data between the portable personal server device and an external device through an external network connected to the communication terminal by the communication terminal's local network connector. The memory stores an operating system for controlling the data processing operations of the local server and the network server. The memory also stores application services executable by the communication terminal and other

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

devices networked to the communication terminal. The memory also stores user specific data. The operating system loads the application services into other memory locations on demand during execution. The messaging API allows the communication terminal to discover and use the application services and access the user-specific data stored in memory as if the application services and data were stored in the communication terminal. The messaging API also facilitates secure communication between the communication terminal and the portable personal server device and between the portable personal server device and other devices networked to the communication terminal. The individual authenticator authenticates an individual based on biometric information, and the control makes the local server and the network server usable only when the individual is authenticated.

A personal portable server device formed in accordance with the claimed invention has a number of advantages. It allows a user to carry his/her own data and unique applications and make them available to others securely over a network connection via any communications terminal, such as a PC. This is both unique and novel. Before the disclosed subject matter was developed, a portable personal server device had not been conceived. More specifically, until the disclosed subject matter was created, no one had developed a personal portable server device combining the unique and novel approaches described and claimed in the current application.

The disclosed portable personal server device can be used to implement a number of different applications that provide application services on behalf of its owner. As it includes its own processing and storage capability, it can provide these functions without the need for any wide area network (such as Internet). Examples of such application services are:

- An *electronic wallet* that stores digital currency and allows secure payment; the owner may configure the application such that larger purchases require biometric

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

acknowledgement, and each transaction may be recorded for further analysis or reporting;

- A *digital notary service* that digitally signs (after biometric acknowledgment, which may acknowledge that a paper version is identical) a document, but also keeps a copy of the notarized digital document for auditing purposes; and
- A *virtual private network proxy* that provides a highly secure encrypted communication channel to a secure network server without revealing that server's address or connection information.

Even though these application services might have been implemented on state of the art hardware devices, the unique capabilities of the portable personal server device allow any number of such application services to be developed and loaded onto the portable personal server device and to be accessed at the same time. Prior solutions were fixed function devices that only implemented one such service or a fixed number of services. Just like traditional fixed function cell phones only provided voice and messaging services, smart phones such as the Apple iPhone now provide an application store where thousands of application services are offered and can be downloaded onto the device. The application service infrastructure, as described and claimed in this application, provides the same level of extensibility for portable servers.

U.S. Patent Application Publication No. 2003/0214779 (Socolofsky)

Socolofsky describes a server for sharing multimedia information (images) across a network to multiple client personal computers (PCs). Specifically, visual data, such as Web pages with pictures and video, are shared and displayed with the help of a Web browser application to the client PCs. While Socolofsky does include server functionality, Socolofsky does not disclose local and network servers for carrying out the functionality of the disclosed local network servers, as described above. Further, as discussed more fully below, Socolofsky

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

does not disclose a messaging API directed to performing the disclosed functions recited above. Also, as recognized in the Office Action, Socolofsky does not disclose an individual authenticator for authenticating an individual based on biometric information nor a control that makes a local server and a network server usable only when an individual is authenticated by an individual authenticator.

The purpose of Socolofsky's server is to share media through a Web server. In contrast, the disclosed subject matter provides a way to transport, secure, and share personal data as well as provide application functions in a small, portable personal server device.

U.S. Patent Application Publication No. 2003/0005336 (Poo)

Poo discloses a portable device having biometric-based authentication capabilities. Other than this disclosure, Poo has little, if any, relevance to the disclosed subject matter.

U.S. Patent Application Publication No. 2003/0157959 (Makela)

Makela describes a server that is used to provide additional data storage for other small portable devices and also allows those portable devices to share data. Even though Makela's technology appears to be somewhat similar in nature to the disclosed subject matter, there are substantial differences both with respect to structure and function. With regard to function, Makela's server is specifically intended for use as a **multi-user** device. In contrast, the disclosed subject matter is specifically targeted to store and manage a **single** person's data and unique applications. The owner of the disclosed device is expected to take the device along as he/she travels. The owner may specifically allow others to access his/her data and applications via biometric authentication. The device is therefore called *personal* server device. This approach is unique and novel.

With respect to structure, Makela does not disclose local and network servers that perform the functions described above or a memory for storing and carrying out the functions

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

recited above. Most importantly, Makela does not disclose a messaging API for carrying out the functions described above. And, of course, Makela does not disclose an authenticator for authenticating an individual based on biometric information and/or a control that makes a local server and a network server only usable when an individual is authenticated.

U.S. Patent Application Publication No. 2002/0186838 (Brandys)

Brandys is directed to a system and method of user and data verification. The data verification method and system employ authenticating biometric information to create a digital signature. More specifically, biometric data is analyzed and carries a random number generator that creates a public key and a private key. The private key is stored in a tamper-resistant component; the public key is transmitted to an external device, such as a computer. Thereafter, messages are digitally signed subsequent to verifying the biometric information that is provided by the user using the private key. Brandys does not disclose a portable personal server device, much less a portable personal server device containing the structural elements and/or functions described above.

Argument

As amended, Claim 1 reads as follows:

> 1. A portable personal server device suitable for functioning as a server when connected to an external network, the portable personal server device comprising:
>
> a local server for processing data between the portable personal server device and a communication terminal equipped with a local network connector suitable for connection to the portable personal server device;
>
> a network server for processing data between the portable personal server device and an external device through an external network connected to the communication terminal by said communication terminal's local network connector;
>
> memory for storing an operating system for controlling the data processing operations of the local server and the network server, the memory also storing application services executable by the

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

communication terminal and other devices networked to the communication terminal, the memory also storing user specific data, the operating system loading the application services into other memory locations on demand during execution;

a messaging API for (i) allowing the communication terminal to discover and use the application services and access the user specific data stored in memory as if the application services and data were stored in the communications terminal and (ii) facilitating secure communication between the communication terminal and the portable personal server device and between the portable personal server device and other devices networked to the communication terminal;

an individual authenticator for authenticating an individual based on biometric information; and

a control that makes said local server and said network server useable only when an individual is authenticated by said individual authenticator.

As noted above, the only independent claim in this application, Claim 1, has been amended to more specifically distinguish the claimed subject matter from the references relied on in the Office Action. In this regard, in a nutshell, Makela describes a portable server. The purpose of the server is to provide extra shared storage to mobile devices. Socolofsky describes a portable server in a book form. The purpose of Socolofsky's server is to share media through a Web server. In contrast, the portable personal service device recited in Claim 1 provides a way to transport, secure, and share personal data as well as application functions. Claim 1 has been amended to clarify these differences. More specifically, Claim 1 has been amended to recite that the claimed portable personal server device includes a memory that stores an operating system (see Figure 2, element 41, and related text for support) that controls the operation of the processing by the local and network servers previously recited in Claim 1. The memory also stores applications executable by a communication terminal to which the portable personal server device is connectable, as well as user-specific data. Claim 1 has also been amended to recite a messaging API (see Figure 4, top element, and related text for support). API is a well-known software term that defines application programming interfaces—in this case, a messaging

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

interface. The messaging API is recited as allowing the communication terminal to discover and use the applications and access the data stored in memory. The messaging API is also recited as facilitating a secure communication between the communication terminal and the portable personal server device. In addition to the added items being shown in the drawings, their functions are described at various locations in the specification of this application.

While applicants agree that there exists prior art, such as Poo, that describes devices specifically designed for the single purpose of biometric authentication of resources and portable servers, such as described by Makela and Socolofsky, the claimed invention is clearly distinguishable from such devices.

Both Makela and Socolofsky only implement one particular protocol for clients to exchange data with the server. In Makela's case, this is a file sharing protocol such as SMB (server message block) or FTP (file transfer protocol). In Socolofsky's case, this is a Web protocol such as HTTP (hyper text transfer protocol). Even though the portable personal server device of the claimed invention could implement those protocols, the described and claimed portable personal server device includes additional software services (see Figure 4), which are neither mentioned nor required by Makela and Socolofsky. These additional software services make the claimed invention materially different from single protocol server devices. First, an operating system is required to load and manage the execution of the application software components that implement the various services. To accomplish this, the operating system needs to manage the available memory (such as RAM, removable storage media, and flash memory; see Figure 2) for application code and data usage. This is a unique challenge due to the scarce memory available on a small and portable device. For sophisticated data management, the portable server device may include a database application. Second, the portable personal server device requires a messaging API in order to accept requests from an external communication

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

terminal such as a PC or other external device. The messaging API allows the requesting terminal (device) to discover which application services are available on the portable personal server device, then sends a data package through the communication interface, unpacks and decrypts the package and breaks the package into the request type and the request's parameters, identifies which application service can handle this type of request (the operating system may need to load that application service), and passes control to that service for processing. The messaging API allows the development of any application on the requesting terminal or device to communicate with any application stored in the described and claimed portable personal server device. In contrast to the servers described by Makela and Socolofsky, which are limited to the single-purpose, fixed data sharing function described in each reference, the described and claimed portable personal server device provides a multi-application server supporting any number of communication protocols through its messaging API. To simplify application development, the messaging API allows the programmer who develops an application for the requesting terminal or device to call upon the application services on the portable personal server device as if the application service is located on the requesting terminal or device. The messaging API also ensures secure communication as it allows an application on the requesting terminal or device to authenticate the portable personal server device. That is, the messaging API makes sure that the requesting terminal device communicates with the proper portable personal server device and not an imposter. In this regard, preferably, the portable personal server device is capable of encrypting any communication between the requesting terminal or device and the portable personal server device to avoid eavesdropping. Also, for security, preferably the portable personal server device also encrypts all its general purpose storage, not just the biometric templates or keys. None of these security functions is described by either the Poo or Brandys references.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

The following table shows the differences in server functionality in more detail.

	Portable Personal Server Device	**Makela**	**Socolofsky**
Users	Personal (single)	Multi-User	Ambivalent
Protocol	Any SOAP	SMB/FTP	HTTP
Server Type	Multi-Application	File	Web
Messaging API	●	○	○
Service Discovery	●	○	○
Programming Transparency	●	○	○

The following table shows the differences in biometric security functionality in more detail.

	Portable Personal Server Device	**Poo**	**Brandys**
Digital Signature	●	○	●
General Purpose Encrypted Storage	●	○	○
Secure Communication	●	○	○
Device Authentication	●	○	○
Programming Transparency	●	○	○

Since none of the references employs a messaging API with the ability to discover application services and provide general purpose storage and secure communication, they simply cannot provide the functionality of the claimed portable personal server device. As a result, applicants submit that Claim 1, particularly as amended, is allowable.

More specifically, applicants respectfully submit that the subject matter of Claim 1, particularly as amended, is clearly allowable in view of the teachings of Socolofsky and Poo. Neither reference, taken alone or in combination, teaches all of the subject matter recited in Claim 1. Further, applicants respectfully submit that there is no basis disclosed in either reference as to why the subject matter of the two references should be combined in any manner. Only the current application suggests any combination. As a result, the rejection of Claim 1

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

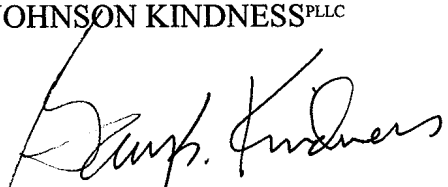
based on the combination of these two references is using impermissible hindsight, not the teachings of the cited references to conclude that the claimed invention is unpatentable.

Since all of the remaining claims in this application (Claims 2–6) are directly or indirectly dependent upon Claim 1 and since none of the other cited and applied references (Makela and Brandys) teaches the subject matter missing from Socolofsky and Poo, these claims are submitted to be allowable for at least the same reason that Claim 1 is allowable. Further, these claims are submitted to be allowable for additional reasons. For example, while Brandys does disclose data encryption and data encryption using biometric information, again, applicants respectfully submit that there is no basis in Brandys, Socolofsky, or Poo to conclude that it would be obvious to combine the subject matter of these references. Only the present disclosure suggests the use of biometric information to provide encryption in a portable personal server device of the type recited in Claim 1. As a result, applicants respectfully submit that Claims 3 and 4 are clearly allowable for reasons in addition to the reasons why the claims from which these claims depend are allowable.

In view of the foregoing amendments and remarks, applicants respectfully submit that all of the claims in this application are allowable. Consequently, early and favorable action allowing these claims and passing this application to issue are respectfully solicited.

Respectfully submitted,

CHRISTENSEN O'CONNOR
JOHNSON KINDNESS^{PLLC}



Gary S. Kindness
Registration No. 22,178
Direct Dial No. 206.695.1702

GSK:mgp/cae/pww

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100